Suplemento especial de computer!dea número 5 • mayo 2001



Seguridad

48 páginas
y más de
15 trucos y
pasos a paso

- Defiéndete de los ataques de intrusos
- Oculta tus ficheros más importantes
- Aprende a proteger tu sistema operativo
- Consigue realizar una navegación más segura por Internet

Las guías fáciles y rápidas para que no te líes con la tecnología

Colección especial de !dea

Bienvenidos

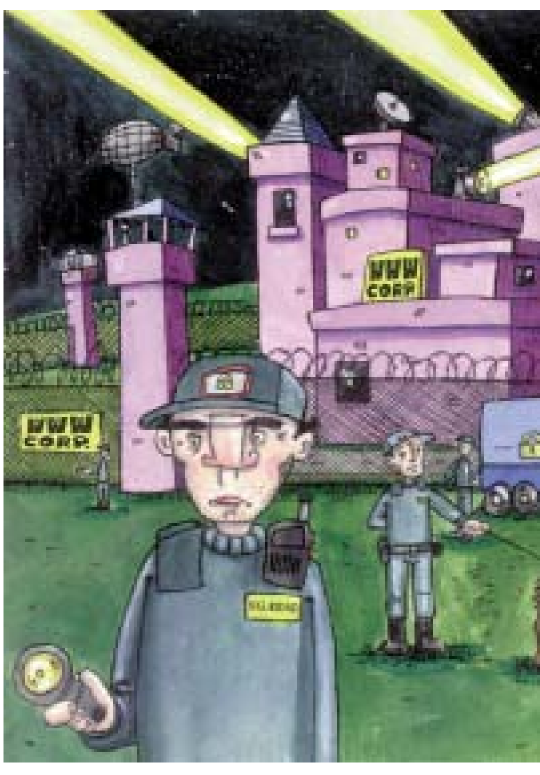
La colección de libros Computer Idea viene a ampliar y profundizar el planteamiento práctico y de utilidad que caracteriza a nuestra publicación. De forma regular, nos acompañará ampliando y desarrollando temas que interesan al gran colectivo de usuarios informáticos: hardware, periféricos, herramientas, software, Internet, comunicaciones, etc. Cada tema es diseccionado minuciosamente para ofrecer pistas y trucos que optimicen la relación entre el usuario y la máquina. Todos estos desarrollos van arropados de conceptos generales y de pasos a paso de las tareas que corresponden en cada situación.
Los pasos a paso se seleccionan en función del provecho que pueden reportar a los lectores, abarcando todo tipo de tareas que pueden interesar tanto a usuarios nuevos como a aquellos más experimentados. Como podréis comprobar, el tono de las explicaciones no encierra gran dificultad. Hemos utilizado un lenguaje lo más claro posible a la hora de explicar las tareas. Que nadie se asuste si se tropieza con algún tecnicismo; en nuestra sección de Vocabulario se explican los términos más frecuentes que resultan imprescindibles para poder entender la jerga informática.

Sumario



Protege tu PC

Hoy por hoy, es imprescindible mantener nuestros equipos protegidos, tanto de posibles ataques externos como de pérdidas de datos causadas por usos indebidos o errores.



Incluso cuando creamos que nuestro aislado ordenador no necesita mayor atención en lo que a seguridad se refiere, en muchas ocasiones estamos bastante confundidos. Aquello de «nuestro ordenador es nuestro castillo» ha dejado de ser verdad gracias a la era de Internet. Eso sin contar con la aproximación de los más pequeños de la casa a nuestros caros equipos. Cada vez que utilizamos una conexión telefónica a redes, abrimos un correo electrónico o permitimos que el «peque» juegue inofensivamente, incurrimos en el peligro de que se introduzcan toda clase de virus o troyanos en nuestros discos duros, o que los iconos y configuración queden corrompidos por una mala utilización del ordenador.

Otras personas, acostumbradas a trabajar frecuentemente delante de una pantalla, están ya sobre aviso del peligro que supone que otras personas accedan a nuestros preciados datos. La pérdida de nuestros imprescindibles ficheros, que en muchas ocasiones han supuesto largas horas de trabajo, es completamente factible, sobre todo si no hemos seguido algunas precauciones básicas en lo que a seguridad del sistema se refiere.

No existe, sin embargo, una solución mágica que acabe con todos estos problemas, más aún si tenemos en cuenta que los productos profesionales suelen tener unos precios exhorbitantes. Además, las soluciones comerciales suelen cubrir tan sólo determinados aspectos de este basto campo, incrementándose el precio aún más.

Por si fuera poco, es raro el ordenador de casa que no tiene Windows 98 como sistema operativo principal. Con una seguridad inexistente y toleracia a fallos que brilla por su ausencia, es harto complicado pretender que nuestro ordenador casero sea un refugio seguro para nuestros datos.

A lo largo de este libro os mostraremos algunos aspectos que todo usuario debería tener

en cuenta a la hora de trabajar con su ordenador de forma segura. Por un lado, en la primera sección veremos algunos aspectos sobre el sistema en general, principalmente hardware. Os mostraremos cómo eliminar el *password* de nuestra BIOS, asegurar la apertura del equipo y utilizar dispositivos que utilizán nuestra huella dactilar para entrar en el sistema.



Por otro lado, la segunda parte trata temas del sistema operativo, como por ejemplo la creación de perfiles de usuario, el registro de Windows o cómo utilizar un antivirus.

En la última sección nos centraremos en la seguridad de los equipos que se encuentran conectados en red o a Internet, desde los aspectos más básicos, y menos conocidos, hasta la utilización de un pequeño Firewall o programas de cifrado que aumentan la privacidad de nuestro correo electrónico.

En algunos de los pasos necesitarás utilizar algún programa. La gran mayoría de ellos los puedes descargar de Internet desde la página, aunque también encontrarás otros que son completamente comerciales.

Fuera de nuestro alcance quedan otras soluciones comerciales. Es precisamente por este motivo por el que no hemos abarcado sistemas operativos como Windows 2000 que, aunque cada vez es más común, todavía queda algo lejos del usuario «de andar por casa». Tampoco nos hemos centrado en soluciones profesionales o en paquetes corporativos, como aquéllos destinados a proteger la seguridad de servidores o los que aplican medidas muy por encima del usuario medio. De igual forma, hemos evitado aquellos paquetes con un enfoque fuera del trabajo «normal», como pueden ser los *tokens* (pequeños aparatos que protegen nuestros certificados digitales, entre otras cosas) o VPN (redes privadas virtuales).

Mención aparte merece la sección dedicada a los programas antivirus. Para mostraros cómo se utiliza uno de estos imprescindibles paquetes de software, hemos utilizado la versión de Panda Platinum. A pesar de tratarse de software comercial, hemos de advertir que todo usuario debería adquirir alguno de los disponibles en el mercado, ya que el riesgo de «contagio» cada día es mayor.

Aquellos usuarios que comparten su ordenador, por ejemplo, con el resto de la familia, encontrarán más de una solución a sus problemas diarios. Personalizar nuestro escritorio, algo tan sencillo como cambiar el fondo de pantalla o nuestros iconos, puede convertirse en una crisis familiar. Con funciones como «perfiles de usuario» cada usuario del ordenador podrá trabajar con él sin interferir en el «espacio de los demás». Lo mismo ocurre con los archivos ocultos y de sólo lectura, en algunos casos esenciales para ocultar el contenido de nuestros discos duros a los ojos más curiosos.

Seguridad a toda costa

Posibilidades básicas de conexión

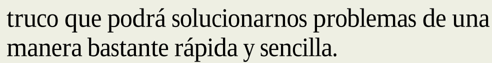
En este primer apartado, daremos unos consejos útiles para la protección y la prevención de fallos en nuestro equipo informático.

Hemos intentado abarcar los aspectos hardware más importantes, entre los que se encuentran la correcta custodia de los dispositivos que se hallan en la carcasa del PC, activación de contraseñas y resolución de problemas BIOS, instalación de un hardware de identificación biométrica y la puesta a punto de los componentes.

Todas las medidas de protección contra el fisgoneo de datos pueden convertirse en algo inútil si se produce un asalto al lugar físico de almacenamiento. Por eso es muy importante contar con la ayuda de candados de cierre si estamos expuestos a un posible robo.

Cuando encendemos nuestro ordenador, la BIOS, que es un chip que se encuentra en la placa madre, realiza una serie de operaciones que son necesarias para el correcto inicio del equipo. Su trabajo comienza antes de la carga del sistema operativo y su cometido es, entre otros, el de recordar la configuración de todos los componentes, como discos duros, unidades de CD-ROM, etc, que se integran. Se puede acceder a ella mediante una interfaz, con objeto de que el usuario pueda variar los parámetros en caso de necesidad de una manera sencilla. Además de todo esto, posibilita la activación de una clave que bloqueará el encendido normal del aparato.

En algunos casos, una mala manipulación de las variables de configuración puede desembocar en un mal funcionamiento del sistema y su restauración puede convertirse en una tarea tediosa si desconocemos la función de alguno de estos parámetros. Mostraremos enseguida un sencillo truco que podrá solucionarnos problemas de una manera bastante rápida y sencilla.



En el apartado de identificación por hardware, nos hemos decantado por la descripción de la implantación de un sistema de reconocimiento de huellas dactilares. Las posibilidades que nos pueden llegar a ofrecer estos dispositivos son de lo más fiables y sus ventajas son indiscutibles. En confrontación a las tarjetas o las simples contraseñas, los rasgos de los que se sirven estos aparatos para llegar a una caracterización son totalmente intransferibles, siempre los llevamos encima y su particularidad los hace eficaces casi al cien por cien.

Este apartado cerrará la sección con una serie de consejos útiles para mantener a punto el ordenador y prevenir posibles catástrofes de corrupción o pérdidas de datos. Hemos entrado en los aspectos referentes al microprocesador, con el reemplazamiento del ventilador y el del posicionamiento y fijación de los discos duros.

BÁSICO

Discos duros bajo llave

Cómo se podrían robar nuestros datos

Toda precaución que tomemos en materia de seguridad respecto a nuestros datos puede desvanecerse si sufrimos un abordaje físico y no consentido a nuestros discos duros.

PASO 1 Una buena compra

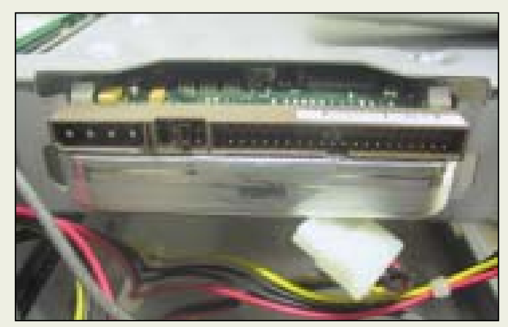
Son muchos los modelos de carcasas que conviven en el inmenso mundo de los ordenadores personales. Tamaños, diseños y estéticas no son los únicos factores diferenciadores que podemos encontrar, y hay aspectos que bien pueden llegar a ser determinantes a la hora de hacer una buena elección. Entre éstos, podemos enfrentarnos con el que se refiere a la seguridad física que en algunos casos se nos brinda, y es que la inclusión de un candado antiapertura salvaguarda la intimidad de los datos que almacenamos en los discos duros.

Dependiendo del fabricante, se puede identificar diferentes técnicas que cumplen, en mayor o menor medida, con el cometido de clausurar las entrañas del PC a intrusos malintencionados. Aunque el *modus operandi* de todos es bien simple, pues tan sólo es necesario un giro con la llave de turno para realizar la apertura, no debemos escatimar en gastos a la hora de hacer la compra.



PASO 2 Proceso de extracción del disco duro

Supongamos que tenemos un ordenador blindado con sendas contraseñas en la BIOS y en el sistema operativo. Éstas cerrarán el paso a nuestros datos a cualquier desconocido que intente encender y arrancar el ordenador desde su lugar físico. Sin embargo, existe una manera bastante sencilla de pasar por alto toda esta estrategia de protección y es evitando el arranque de la BIOS y del sistema operativo. ¿Algo complicado? Sin las medidas adecuadas veremos que no. El proceso es bien sencillo, pues tan sólo tendremos que desconectar el disco duro en el que se almacena la información que se pretende fisgonear. Un destornillador de estrella será la única herramienta necesaria que nos permitirá llevar a cabo la acción.



Una vez desconectada la unidad, es posible determinarla en modo esclavo por medio de los *jumpers* o configuradores. Éstos son unos plásticos que realizan contactos estratégicos y que informan al sistema de su modo de operación. La información de sus posibles posiciones viene indicada junto con las características y el número de serie del disco, por lo que resulta una tarea relativamente sencilla su consecución. El objeto de nombrar al disco duro como esclavo es el de que pueda convivir simultáneamente con otro en una misma conexión.

PASO 3 Implantación de la información en otro equipo

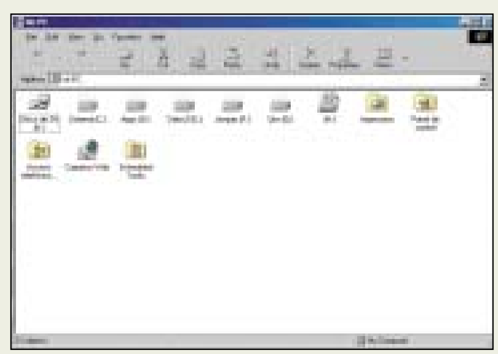
Efectivamente, para poder hacerlo funcionar, tendremos que conectarlo en otro ordenador



diferente, enchufarlo a la faja IDE correspondiente y a la alimentación, y no habrá mas misterios para su uso. Al encender el ordenador, será necesario introducirse en el menú de la BIOS y dar de alta el disco duro que fisgonear. Esta fase también es de lo más sencilla, pues la gran mayoría de los modelos de placas base incorporan una utilidad, HDD detect, que detecta e instala en pocos segundos el dispositivo.

PASO 4 Operando con los datos

Bien, una vez que el equipo ha sido arrancado, podremos ver que dentro de la ventana denominada *Mi PC* contamos con una unidad más, la cual puede ser inspeccionada con toda facilidad. Podremos navegar, buscar ficheros determinados desde el propio buscador de Windows y copiar la información al otro disco duro. Como el sistema operativo se carga desde



la otra unidad, no será necesario introducir ningún tipo de contraseña y los datos estarán de una manera totalmente transparente. Utilizar un programa de encriptación de datos puede solventar de manera efectiva este problema, ya que así la información que se pueda extraer será inteligible. Aún así, si el operador es alevosamente malintencionado, puede borrar de manera totalmente definitiva datos de vital importancia.

Restaurar los sistemas

Realizar el proceso inverso evitará que salte cualquier posible indicio de sospecha del robo de información, lo que puede suponer una auténtica catástrofe de intimidad o confidencialidad de datos. Como hemos visto, esta práctica es bastante sencilla y se puede realizar en pocos minutos.

Por otro lado, no debemos descartar esta operación como una posible solución de emergencia para acceder a datos de manera alternativa en el caso de que desconozcamos las contraseñas y nos sea imprescindible conocer rápidamente una información determinada.



Una *password* en la BIOS

Salvaguarda todo el sistema de personas no autorizadas

Una de las formas mas fiables de denegar el acceso a un equipo informático es la de activar la contraseña de la BIOS, ya que su desconocimiento impedirá realizar cualquier tipo de operación a un usuario no autorizado.

PASO 1 Accediendo a la interfaz de la BIOS

Dependiendo de la placa base, y más concretamente del modelo de BIOS que tengamos, varía la manera de entrar en la interfaz. Se puede averiguar de manera sencilla, pues siempre que



encendemos el ordenador un mensaje nos informa de la tecla o teclas que debemos pulsar para su ejecución. El mensaje suele ser del tipo *Press DEL to enter SETUP*. Este *SETUP* no es ni más ni menos que la mencionada interfaz. Generalmente la tecla suele ser la denominada «DEL» (*delete*, borrar), que en los teclados en castellano se corresponde con la famosa «Supr», o en su defecto «F2». Esta operación debe hacerse nada más poner en marcha el equipo, antes de que empiece el inicio de Windows.

En cualquier caso, y si tenemos algún problema, podemos utilizar un truco para sacarnos de toda duda: si colocamos las dos manos sobre el teclado, de tal forma que presionemos un gran número de teclas, provocaremos un error que nos dará un acceso directo.

PASO 2 Estableciendo la contraseña de acceso

Antes de seguir será conveniente saber que la información que aquí se guarda es de vital importancia para el funcionamiento, y que una incorrecta manipulación puede afectar de manera determinante al equipo. Por eso recomendamos, a menos que el usuario sepa lo que hace, no cambiar ninguna variable con la que nos podamos encontrar.

La forma de operar dependerá del modelo, pero es una tarea sencilla, ya que podremos identificar fácilmente un apartado que tenga que ver con la seguridad (*Security*) o contraseñas (*Passwords*). Entrando en el menú correspondiente tendremos la opción de dar de alta las claves, lo cual tendremos que realizar por dos veces para evitar la posibilidad de que introduzcamos una secuencia errónea.



PASO 3 Guardar los cambios de la configuración

Antes de proseguir deberemos guardar los cambios que hemos realizado en la BIOS. En algunos casos, tenemos la posibilidad de movernos por el menú y seleccionar la opción *Exit*, y en otros tendremos que salir a la pantalla principal presionando de manera repetida la tecla de escape «Esc». A continuación se nos preguntará si realmente deseamos salir de la aplicación guardando los cambios efectuados, a lo que tendremos que responder que sí, pulsando la tecla «Y», que viene a significar *yes*. Si no estuviéramos seguros de haber llevado a buen puerto todo esto, lo mejor será descartar los cambios presionando «N», pues así evitaremos posibles conflictos de configuración.



PASO 4 Comprobar el correcto funcionamiento

Después de todo esto el equipo se reiniciará de manera totalmente automática, y comenzará el arranque aparentemente normal. Sin embargo, y si todo ha ido bien, antes de que se produzca la carga de Windows, un cuadro de diálogo saltará con el



mensaje *Enter password* (introduzca la contraseña). Para seguir el proceso corriente necesitaremos teclearla, ya que de otra forma no podremos avanzar, quedando así el acceso totalmente denegado. Se imposibilitará la carga de otro sistema operativo mediante un disquete de arranque y, lo que puede ser aún más importante, se impedirá cualquier operación con el o los discos duros, por lo que será imposible eliminar cualquier dato que contuviera. Si algún día quisiéramos cambiar la clave de acceso, no tendremos más que repetir toda la operación sin introducir ningún carácter en el cuadro de inserción de *Password*.

Recuperar la contraseña

Aunque muchos usuarios y, sobre todo, compañías, ven con malos ojos páginas como las que os comentamos en este breve cuadro, lo cierto es que pueden ser muy útiles para reforzar la protección de los propios usuarios. En la web que aparece en la imagen, *www.vanhackez.com/archivos/Password_Crackers/BIOS/*, es posible obtener el software necesario para recuperar la contraseña de la BIOS en caso de que la hayamos perdido. Pese al nombre del *site*, que recordará vagamente al de algún pirata inglés, la utilidad de la página es indiscutible.



BÁSICO

Resetear la BIOS

Si olvidas tu *password*, siempre te queda esta opción

Siempre nos puede ocurrir cualquier eventualidad; y si nos puede ocurrir, nos ocurre. Pero también tenemos una solución para cada problema.



PASO 1 Un ojo al manual

En el caso de que hayamos olvidado las claves de nuestra BIOS, no nos quedará más remedio que «resetearla». Se trata de un proceso bastante sencillo, no obstante debemos ser precavidos ya que implica abrir el ordenador y acceder directamente a la placa madre. En primer lugar buscaremos en el manual de la placa base del equipo la localización del *jumper* que borra la memoria CMOS del equipo, que es donde se almacenan los valores de la BIOS. Normalmente encontraremos este pequeño interruptor identificado como *CMOS Clear*. Consultando esta documentación también debemos averiguar en qué posición colocar el *jumper* para el funcionamiento normal de la placa.

PASO 2 Abrir el equipo

A continuación tendremos que armarnos con un destornillador y abrir el equipo. Es muy importante que previamente desconectemos el cable de alimentación. Aunque pueda parecer algo completamente obvio, no es en absoluto trivial, ya que aunque el ordenador esté apagado la corriente eléctrica llega hasta la placa y podemos causarle graves daños.



PASO 3 El *jumper*

Con el ordenador abierto localizaremos el *jumper* sobre la placa, con cuidado para no desenchufar los cables que están conectados a ésta. En el caso de que sea necesario quitar alguno de ellos, debemos recordar dónde se encontraban enchufados **y en qué posición**. Dado que algunas cajas son bastante inaccesibles, puede que





sea completamente necesario desconectar varios cables para tener un mejor acceso a la superficie de la placa madre.

PASO 4 Devolverle la vida

Tal y como se nos indica en el manual de la placa, tendremos que extraer la pequeña pieza de plástico y volver a ponerla, en la posición adecuada. Tras esperar unos segundos, colocaremos de nuevo la pieza en su posición original, que permite a la BIOS mantener los valores en la memoria. Si el acceso a la pieza es muy complejo, puede ser recomendable utilizar unas pequeñas pinzas, ya que suelen ser piezas de pequeño tamaño difíciles de manipular, especialmente si los cables dentro de la caja no permiten meter la mano con comodidad. Otra consideración, sobre todo si utilizamos las pinzas, es tener cuidado para no dañar la superficie de la placa ya que en ella se encuentran delicadas pistas serigrafiadas.



Instala un detector de huellas dactilares

La forma mas efectiva de identificación

La biometría es una excelente solución para controlar el acceso de personas autorizadas a los datos de nuestro ordenador, o en su caso denegarlas.

PASO 1 Implantación del software

Para que el lector de huellas pueda funcionar de manera correcta, es necesario que se instale un software que, proporcionado por el fabricante, sirva de interfaz entre el escáner, el ordenador y los usuarios. Esta operación es de lo más sencilla y, aunque podemos encontrarnos con pequeñas diferencias dependiendo de cada modelo, no tendrá misterio alguno seguir los pasos del asistente. Después de realizar esta tarea, se nos pedirá que reiniciemos el PC para que los cambios producidos surtan efecto.

PASO 2 Conectando el lector

Son muchas las formas, tamaños y conexiones de los escáneres de huellas que habitan en el mercado. Desde tarjetas PCMCIA para portátiles, hasta los más comunes con enlace USB, tienen un mismo modo de operación tanto en su manejo como en su ensamblado. Después de enchufarlo, el PC reconocerá inmediatamente su presencia y actuará en consecuencia para lanzar el software de gestión de huellas, que constituirá una base de datos de los usuarios con privilegios de acceso.

PASO 3 Introducción de las huellas

En este momento, tendremos que empezar a dar de alta las lecturas de las yemas de los dedos de aquellas personas que deseamos tengan acceso a la información. El primero de ellos tendrá que ser el administrador,



quien tendrá la posibilidad de crear nuevos registros o eliminarlos de manera permanente. La propia interfaz del programa tendrá un asistente que nos informará de los pasos que seguir.
Ahora tendremos que posicionar uno de nuestros dedos sobre el escáner por lo menos tres veces consecutivas, para que se tenga una lectura totalmente fiable, e introducir el nombre de usuario correspondiente. La mayoría de los productos nos permiten introducir más de un dedo, cosa bastante interesante, ya que si un día sufrimos algún percance que nos impida utilizarlo (por estar vendado), podremos utilizar la otra para mantener el acceso.

PASO 4 Gestión del administrador

Si reiniciamos ahora el ordenador, podremos observar que al iniciar Windows se nos pide que ubiquemos un dedo sobre el identificador. Si el usuario no está dado de alta en la base de datos, el acceso le será denegado impidiéndole cualquier tipo de operación.
Para dar de alta a una persona, tendrá que ser el administrador quien se identifique y arranque el software de gestión.



BÁSICO

Prevención de fallos del hardware

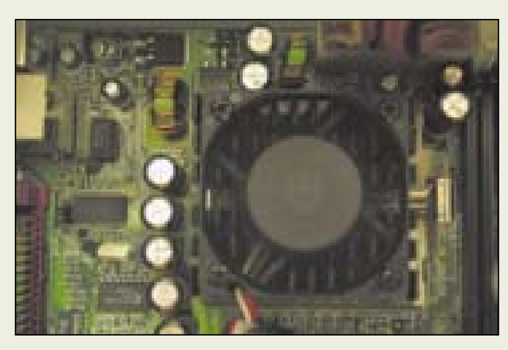
Pon a punto los componentes de tu PC

Un mal funcionamiento del ordenador puede causar errores y pérdidas importantes de información. A continuación os damos unos consejos para prevenir averías.

PASO 1 Cambiar el ventilador del procesador

El ventilador que se encuentra situado en nuestro «micro» no está ahí de adorno. Es el encargado de mantener a baja temperatura el componente, algo del todo necesario para que pueda realizar de manera correcta su cometido, y que además alargará su esperanza de vida. Un mal funcionamiento de éste puede traducirse en un molesto zumbido provocado por la acumulación de suciedad, lo que impide realizar su misión. También puede provocar un calentamiento excesivo del procesador, que se manifestará con continuos «cuelgues» del sistema, ralentización de procesos, corrupción de datos y hasta causarle deterioros irreparables.
Para cambiar al ventilador dañado procederemos primeramente a desconectar el cable de suministro





eléctrico, para evitar cualquier posible accidente. Posteriormente abriremos la carcasa con la ayuda de un destornillador de estrella y lo identificaremos fácilmente. Para extraerlo será necesario desensamblar el «micro». Si tiene formato *slot* presionaremos hacia abajo las pestañas laterales, y posteriormente lo sacaremos tirando de él. Si por el contrario contamos con uno de forma *socket*, buscaremos una palanca que incorpora el zócalo y la retiraremos; ahora saldrá fácilmente.
El ventilador se adhiere por diferentes sistemas de sujeción, que dependerán de cada modelo. Generalmente tienen unos enganches de plástico o en su defecto una lámina de metal que fija los dos componentes.
En algunos casos bastará una buena limpieza para restaurarlo, lo cual se puede hacer con un trapo seco y un destornillador. Si esto no fuera suficiente, procederemos a su cambio realizando todos los pasos de manera inversa para su colocación.

PASO 2 Fijar los discos duros

Según las especificaciones de todos los fabricantes, los discos duros están diseñados para trabajar en posiciones paralelas o de 90 grados con respecto al suelo. Al ser dispositivos electromecánicos, están sujetos a posibles averías de manera irrevocable que son provocadas por las continuas vibraciones a las que están sometidos. Por eso es imprescindible cerciorarnos de que están fuertemente fijados al chasis de la carcasa, así como de que tengan una correcta ubicación. Un reajuste periódico será beneficioso para la durabilidad del sistema, y por extensión de la información que en ellos se guarda.



Un seguro para el sistema

Protege el corazón de tu PC de sustos inesperados

Afrontamos el problema de seguridad desde el propio sistema operativo o con programas especializados que aumentarán el nivel de protección y prevención.

Dentro de lo que engloba las posibilidades de protección y prevención de posibles fallos, corrupción de datos, operaciones ilegales o fisgoneo de información, de lo que es el sistema operativo, mostramos una serie de estrategias que a buen seguro se ajustarán a las necesidades que tengamos en cada momento.
Podemos ver que los niveles de seguridad, en este aspecto, tienen diferentes escalones de fiabilidad, y en muchos casos una buena política que encaje en las características de uso particular no tiene porqué suponer engorrosas tareas y grandes consumos de recursos.
Intentar cubrir todos los campos, en cuanto a materia de seguridad, se escaparía en el horizonte de nuestras miras, por lo que hemos intentado abarcar los flancos más importantes por los que nos podemos cubrir.
Así, vamos a dirigirnos a apartados de diversa índole, desde operaciones que nos permite el propio Windows hasta programas adicionales especializados que nos aportan un mayor control sobre el propio ordenador.
Los procesos de protección de documentos nos aliviarán de sus posibles pérdidas en el caso, intencionado o no, de que se intenten modificar.
Así mismo, aprenderemos a ocultar ficheros para evitar posibles fisgoneos, tanto si se intentan realizar desde el propio ordenador, como desde otro PC que se encuentre conectado.
Conoceremos un tipo de programa que constituye todo un auditor de operaciones, capaz de almacenar y mostrar de una manera totalmente discreta todas las tareas que se realicen des-



de la unidad. Esto será de gran importancia para aquellos padres preocupados por las actividades que sus hijos realicen delante de la máquina. Contraseñas, páginas web visitadas, etc., quedarán plasmadas en un gestor fácilmente interpretable.
Así mismo veremos una serie de políticas de operación, que nos evitarán muchos sustos. Copias de seguridad de archivos, del registro de Windows y personalización de los entornos serán complementos para contribuir a la seguridad, tanto de la intimidad como de la prevención de la corrupción de datos.

BÁSICO

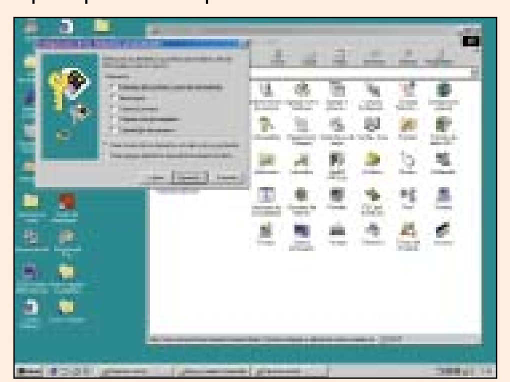
Personaliza el escritorio bajo una contraseña

Controla el acceso a los datos desde Windows

Con este sistema podremos crear perfiles de usuarios para que varias personas que utilicen un mismo ordenador puedan mantener su propia configuración y no compartir sus archivos.

PASO 1 Añadiendo un nuevo perfil de usuario

Si nos dirigimos al *Panel de control* (en la ruta del menú *Inicio/Configuración*) podemos ver un icono denominado *Usuarios*. Pulsando sobre éste, se lanzará un asistente que nos llevará paso a paso por toda la operación. Primeramente intro-



duciremos el nombre de usuario, para posteriormente añadir una contraseña asociada.

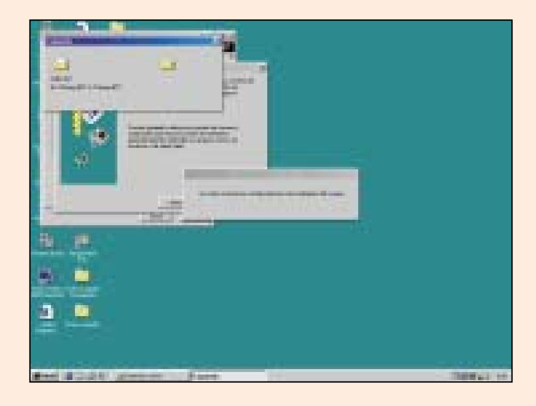
A continuación nos aparecerá una ventana con todas las posibilidades de personalización que se nos permiten. Éstas son: *carpetas del escritorio y menú de documentos*, *menú Inicio*, *carpeta Favoritos*, *páginas web descargadas* y *carpeta Mis documentos*.

En la parte inferior se permite realizar la opción de crear copias de los elementos actuales y de su contenido, lo que significa que todos los objetos que se encuentren en la actualidad en el escritorio permanecerán para el perfil creado.

PASO 2 Finalizando y «reseteando» el ordenador

Después de todo esto, y para poder iniciar una sesión como usuario nuevo, se reiniciará el ordenador. Si elegimos anteriormente la opción de *Crear copias de los elementos actuales y de su contenido*, se procederá a generar los nuevos ficheros independientes, para lo cual habrá que esperar durante unos pocos minutos.

Esta operación se puede realizar cuantas veces queramos (o las que nos permita el espacio en el disco duro).



PASO 3 Creación de un nuevo usuario

Para dar de alta a un nuevo operador, se procederá de la manera anteriormente descrita, pero ahora encontramos una pequeña variante, la del administrador de usuarios. Desde aquí podremos operar haciendo clic en *Nuevo usuario* (para crearlo), en *Eliminar* (para hacer lo propio) o en *Hacer una copia* (para duplicar el perfil). Este gestor nos permitirá cambiar las contraseñas y las configuraciones de cada una de las personas que estén dadas de alta en el sistema operativo. Para modificar las claves, pincharemos en el usuario deseado y nos saltará un nuevo cuadro en el que será necesario rellenar los campos de *Contraseña anterior*, *Nueva contraseña* y *Confirmar nueva contraseña*.



Para variar las configuraciones, pincharemos sobre esa opción y modificaremos los puntos que deseemos.

MEDIO

Oculta tus datos

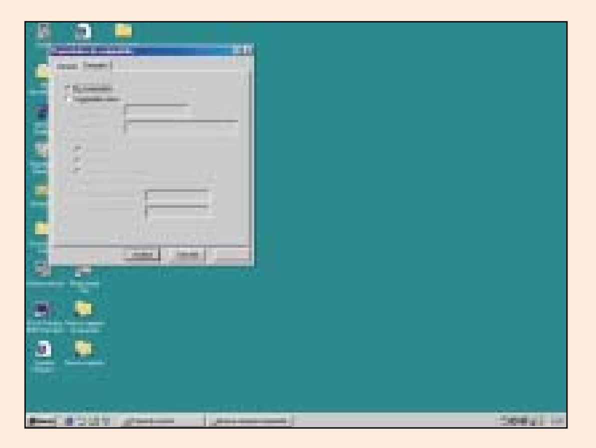
Cómo impedir que vean tus carpetas

Aquellos que dispongan de una pequeña red local y estén habituados a utilizar recursos compartidos para el intercambio de información entre equipos, conocerán las posibilidades que ofrece la protección por contraseñas; pero hay más medios para crear seguridad.

PASO 1 Una carpeta nueva

Existe otra forma de evitar que ojos curiosos se entrometan en nuestros directorios compartidos, consistente en evitar que el nombre de los recursos se visualice en el explorador de cualquier otro equipo que examine la red. Para ocultar uno de estos recursos utilizaremos el mismo método que emplea el propio sistema para evitar que se muestren directorios destinados a servir únicamente a administradores o a otros propósitos como la conexión remota de programas. En primer lugar tendremos que crear una carpeta en nuestro disco, pulsando allí donde queramos crearla con el botón derecho del ratón y escogiendo la opción *Nuevo* y *Carpeta*.



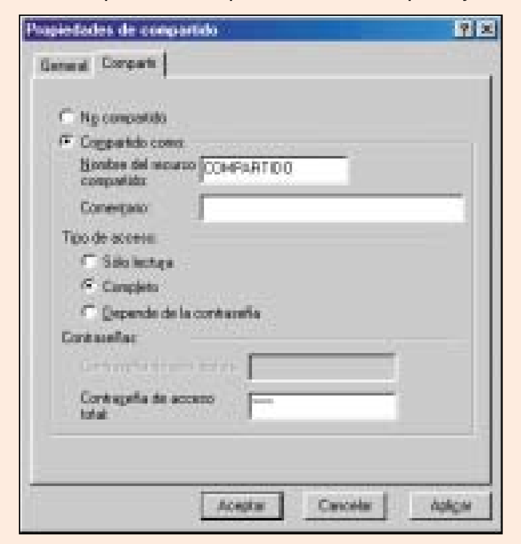


PASO 2 Modificar opciones

Una vez le hayamos asignado a la carpeta el nombre que más nos convenga, abriremos las opciones del icono, pulsando con el botón derecho sobre éste y seleccionando la opción compartir. Aparecerá un nuevo menú en el que podemos modificar las opciones de seguridad de la carpeta, como por ejemplo las contraseñas de acceso de lectura o escritura, así como el nombre del recurso compartido. Encontraremos estos parámetros bajo la pestaña *Compartir* de la ventana.

PASO 3 Tipo de acceso

Como hacemos con todos aquellos recursos que necesitamos compartir, pulsaremos sobre *Compartido como*, lo que habilitará el resto de las opciones que aparecen en este cuadro de diálogo. Seleccionaremos a continuación el tipo de acceso que vamos a permitir a esta carpeta, ya



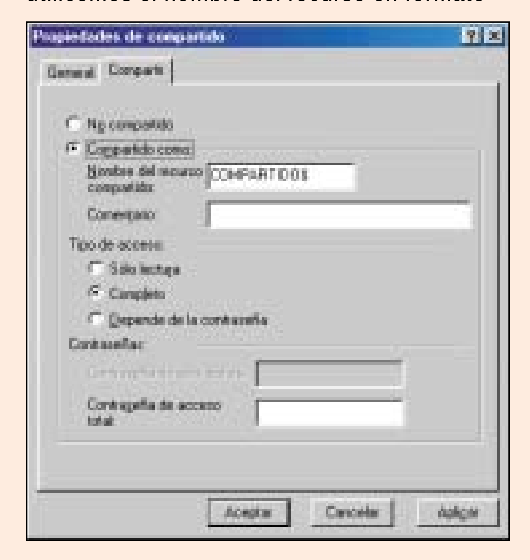
sea *Sólo lectura*, *Completo* o en función de la contraseña. En caso de establecer algún tipo de contraseña especificaremos ésta en los recuadros apropiados.

Esconde tu disco duro

Así como hemos ocultado ficheros en este paso a paso, es posible esconder una parte de nuestra memoria de almacenamiento, que podemos «mostrar» como un disco duro. Hay diversos programas capaces de hacer esto; uno de ellos, Scramdisk, es posible bajárselo gratuitamente de su página web */www.scramdisk.clara.net/*. En el interior de la revista encontrarás un paso a paso en el que te explicamos cómo hacerlo.

PASO 4 Ocultarla a ojos ajenos

La última fase consiste en asignarle al recurso un nombre que el resto de los clientes de la red de Windows consideren administrativo y, por lo tanto, eviten mostrarlo en pantalla. Para ello, dentro del *Nombre del recurso compartido*, escribiremos el nombre deseado, seguido del carácter $. Este tipo de nombres no se mostrarán en ningún explorador de los sistemas de Microsoft (incluso Windows 2000 parece ignorarlo). Para acceder a esta carpeta será necesario que utilicemos el nombre del recurso en formato



UNC. De esta forma, si el equipo se llama "Miequipo" y la carpeta compartida "Compartido$", para acceder al equipo tendremos que abrir un *Explorador de Windows* y escribir en su barra de direcciones *\\Miequipo\Compartido$*. Una vez dentro veremos todos los ficheros y subcarpetas; no obstante, aquellos clientes que no conozcan este «truco» no los verán ni se percatarán de su existencia. Por supuesto, para aplicar estos cambios tendremos que pulsar sobre el botón *Aplicar* y posteriormente *Aceptar*.



Personalizar la seguridad

Editor de planes para hacer modificaciones al gusto

Windows posee una serie de posibilidades ocultas, que tenemos que «descubrir» para poder realizar cambios.

PASO 1 Un programa nuevo

Para personalizar algunos parámetros, que de otra forma se encontrarían ocultos a nuestros ojos, tendremos que emplear una herramienta que no se instala por defecto con Windows 98, sino que requiere que nos dirijamos al *Panel de Control*. Dentro de esta carpeta abriremos el icono *Agregar o quitar programas*. En la nueva ventana, seleccionaremos la pestaña *Instalación de Windows* y pulsaremos el botón *Utilizar disco*. En el diálogo que se nos presentará escribiremos la ruta *\tools\Reskit\Netadmin\Poledit* de nuestra unidad de CD, con el CD-ROM de Windows 98 instalado. Aparecerán los programas que podemos instalar, escogiendo esta vez el *Editor de planes de sistema*.



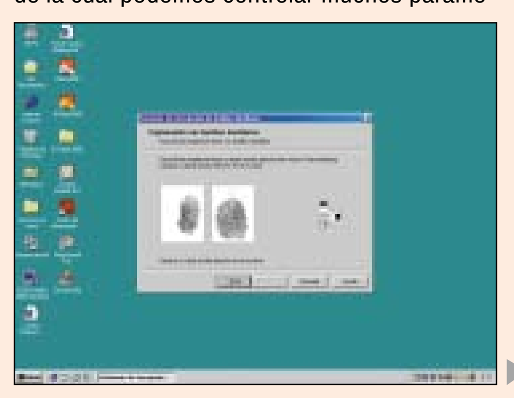
PASO 2 El editor de planes

Podremos abrir el nuevo programa instalado desde el botón de *Inicio*, en los menús *Programas*, *Accesorios*, *Herramientas del sistema* y finalmente *Editor de planes del sistema*.



PASO 3 Cambios en el registro

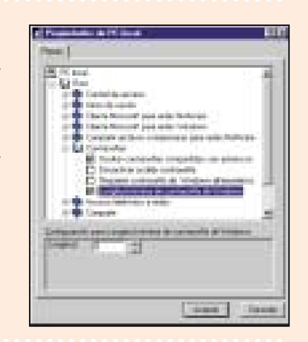
Una vez iniciado el programa, aparecerá una ventana en blanco desde la cual podemos controlar muchos paráme-



tros que en principio parecen ocultos. Para acceder a estas opciones tan sólo tendremos que abrir el menú *Archivo* y seleccionar *Abrir registro*. Esto nos permitirá realizar los cambios oportunos directamente sobre el registro de Windows.

PASO 4 Libros de opciones

Si pulsamos sobre *PC local* podremos ver las propiedades de nuestro ordenador. Éstas se encuentran estructuradas en varios libros, compuestos de diferentes opciones. Así, por ejemplo, bajo el libro *Contraseñas* se encuentran opciones como *Ocultar contraseñas compartidas con asteriscos* o *Longitud mínima de contraseña de Windows*. En esta última tenemos un ejemplo de una política en la que es necesario establecer algún valor, en este caso la longitud mínima. Encontraremos que existen varias opciones en las que podemos definir múltiples valores según sea necesario.

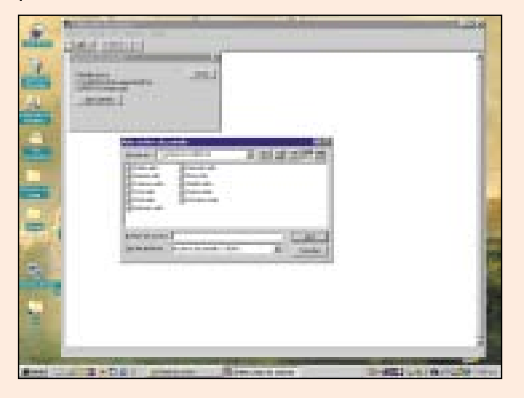


PASO 5 Validar las modificaciones

Para almacenar los cambios realizados solamente tendremos que pulsar sobre el botón *Aceptar*. Las modificaciones se darán por válidas cuando abramos de nuevo el menú *Archivo* y seleccionemos la opción *Guardar*.

PASO 6 Otras posibilidades

Pero no son éstas las únicas opciones disponibles. Tendremos acceso a diferentes plantillas de valores desde el menú *Opciones*. Dentro de este dialogo, pulsando sobre *Abrir Plantilla* se nos dará la oportunidad de acceder a nuevas plantillas (con extensión ADM). Encontraremos más de estos ficheros en la misma carpeta desde la que instalamos el programa. Alguna de las más interesantes es *shellm.adm* que nos permite el acceso a opciones sobre políticas adicionales de la interfaz de órdenes. Tras abrir este archivo tendremos que recurrir otra vez al menú *Abrir Registro*.



PASO 7 Modificar las opciones de usuario

Al igual que es posible modificar las opciones referentes al equipo, también tenemos la oportunidad de modificar aquellas dependientes del usuario, seleccionando el icono *Usuario local*. Se trata de una opción más que recomendable para personalizar nuestro escritorio.



BÁSICO

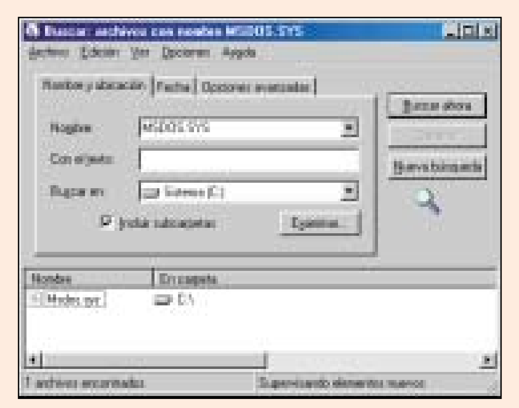
Evitar la interfaz de comandos

Cómo soslayar otra forma de intromisión

Una pequeña medida para evitar que cualquiera entre en nuestro sistema utilizando la interfaz de comandos es precisamente evitar el arranque de nuestro ordenador utilizando la tecla «F8» cuando aparece el menú de inicio.

PASO 1 El fichero msdos.sys

Para ello, tendremos que editar los parámetros que se encuentran en el fichero de configuración msdos.sys. Este archivo se encuentra en el directorio raíz de



nuestro disco duro, no obstante no tendremos acceso a él, normalmente incluso ni lo veremos. Para localizarlo lo primero que tendremos que hacer será localizarlo en el disco, para lo cual utilizaremos el menú de búsqueda de archivos que se encuentra en el menú de *Inicio*, introduciendo en la casilla correspondiente msdos.sys.

PASO 2 Cambiar sus atributos

Habiendo localizado el archivo, será necesario que deshabilitemos los atributos que, de alguna forma, lo protegen. Para esto pulsaremos sobre él con el botón



derecho del ratón, y escogeremos la opción *Propiedades*. Dentro de la nueva ventana pulsaremos sobre *Sólo lectura* y *Oculto*, oprimiendo a continuación el botón *Aplicar* y finalmente *Aceptar*.

PASO 3 El Bloc de notas

Para la edición del archivo pulsaremos nuevamente sobre él, pero esta vez seleccionaremos la opción *Abrir con...*. Ésta dará paso a un nuevo menú en el que tenemos la oportunidad de seleccionar la apli-

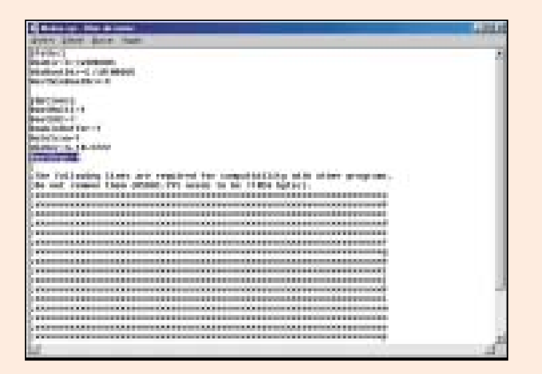




cación con la que realizar la edición del fichero. Lo más oportuno es que nos decantemos por el *Bloc de notas*.

PASO 4 Edición del fichero

Por fin tenemos ante nosotros el contenido del fichero. Es recomendable que no editemos más que aquello que conozcamos perfectamente, ya que de otra forma nuestro sistema puede dejar de iniciarse con normalidad. Aunque la recuperación de un fallo en este fichero es bastante sencilla (basta con copiarlo o crearlo de nuevo utilizando un disco de arranque), es mejor ser precavido. Para evitar la utilización de las teclas de función durante el arranque, que dan paso a arrancar en modo *Sólo símbolo del sistema*, tendremos que añadir una



línea de código como *BootKeys=0* bajo el epígrafe [Options]. Volver a habilitar esta función es tan sencillo como eliminar la línea o sustituir el número 0 por un 1. Si además añadimos *BootMenu=0* nos aseguramos de que es imposible acceder al menú si no es utilizando las teclas de función, previamente desechadas. Al cerrar el programa se nos pedirá confirmación para guardar los cambios; deberemos pulsar sobre el botón *Aceptar*.

PASO 5 Devolverle sus atributos

Finalmente tendremos que repetir el segundo paso, pero esta vez a la inversa. De esta forma devolveremos el fichero a su estado «protegido» original, es decir, con los atributos de *Oculto* y *Sólo lectura*. Se trata de una medida que no conviene



dejar de lado ya que, como hemos mencionado, corromper este fichero dará lugar al fallo de nuestro sistema. Además, impedimos que por accidente éste cambie de localización en nuestro disco o que sea modificado por algún programa peligroso.

BÁSICO

Crea copias de seguridad de tus trabajos y programas

El *backup* permite salvaguardar los datos

Todas las precauciones que podamos tomar como protección de datos, son pocas. Por eso os enseñaremos a prevenir posibles desastres, mediante el hábito de realizar copias de seguridad periódicamente.

PASO 1 Identificar los ficheros importantes

El primero de los pasos que seguir para realizar todo este proceso es el de la identificación de los archivos cuya pérdida supondría una catástrofe. Sería del todo inútil crear copias de ficheros del sistema, a los que siempre podremos recurrir en caso de emergencia directamente en el CD de instalación. Es importante dedicarle todo el tiempo que sea necesario a esta operación y asegurarnos que no olvidamos ni uno solo de los componentes importantes.
Una manera organizada de agrupar todos los documentos es la de crearnos una carpeta denominada, por ejemplo, *Copias*, y operar de la siguiente forma: cuando identifiquemos un fichero o una carpeta importante, pinchamos con el botón derecho del ratón y nos deslizamos hasta *Copiar*.





PASO 2 Comenzar a hacer las copias

A continuación, nos dirigiremos al lugar donde creamos la carpeta *Copias* y pincharemos sobre ella con el botón derecho del ratón nuevamente. Veremos que ahora se despliega una opción que se denomina *Pegar*, que será la que tenemos que seleccionar. Si entonces abrimos la carpeta, podemos ver que en ella se encuentra copiado el archivo que elegimos en un principio. Esta operación la realizaremos cuantas veces sea necesario, inspeccionando todas las partes del disco duro.

PASO 3 Usar un compresor

El gran sacrificio que supone hacer una de estas copias es que el espacio del disco duro se ve menguado, pues hemos duplicado algunos archivos. Por eso es conveniente comprimirlos para reducir al máximo el tamaño de la carpeta que creamos en la fase anterior. Para ello necesitaremos la ayuda de un programa compresor de datos, que agrupará la carpeta en un solo archivo con unas dimensiones sensiblemente inferiores. Nosotros hemos optado por la utilización de WinZip, ya que es uno de los programas más usado en el mundo del PC. La versión de evaluación de este programa lo podemos encontrar en la dirección de Internet *www.winzip.com*.

PASO 4 Comprimir la carpeta

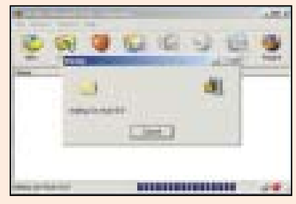
El primer paso será el de abrir el programa haciendo doble clic sobre su icono. Se nos mostrará una ventana vacía. El



paso siguiente será el de pinchar sobre la carpeta de las copias y arrastrarla hasta la citada ventana vacía.

PASO 5 Ubicando el fichero comprimido

Aparecerá un cuadro de diálogo, en el que tendremos que indicar el lugar donde se ubicará el fichero finalmente comprimido. La ruta se inscribirá en la parte superior, en el hueco denominado *Add to archive*. Una



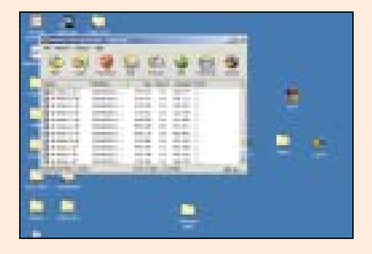
vez que hemos introducido el sitio, presionaremos el botón con nombre *Add*. Después de unos segundos, podremos ver que el archivo ha sido guardado en la ruta especificada.

PASO 6 Mejor en unidades extraíbles

En estos momentos estamos ya preparados en el caso de que suframos una pérdida de información, pues aunque la copia de seguridad no se actualice, siempre podremos recuperar gran parte del trabajo que teníamos hecho antes de la «catástrofe». Lo ideal de este proceso sería almacenar la copia en un disco duro o en una unidad extraíble independiente, pues de esta manera, si se sufren daños en todo el disco, podremos restaurar los cambios. Todo este proceso deberá realizarse de manera periódica, con el fin de que si nos coge por sorpresa el problema, perdamos el menor número de datos posibles.

PASO 7 Recuperación de los datos

En el caso de que deseemos hacer la recuperación, necesitaremos arrancar la aplicación compresora. Después de esto pincharemos sobre el icono del archivo comprimido, y lo desplazaremos hasta la ventana del programa de forma similar a cuando realizamos la tarea inversa. Después de unos segundos, veremos que aparecerán los archivos que habíamos comprimido. Para recuperarlos, tan sólo habrá que seleccionarlos y llevarlos fuera de la ventana, por ejemplo a otra carpeta.



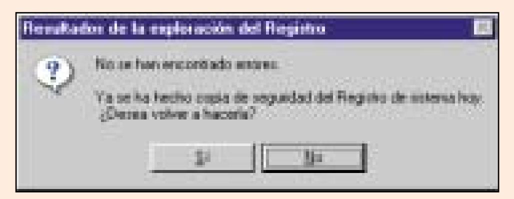
Copia de seguridad del Registro

Uno de los elementos clave del sistema a salvo

Dado que el Registro de Windows es una de las partes más delicadas del sistema, conviene tener una copia de seguridad como prevención ante desastres.

PASO 1 Archivos de seguridad

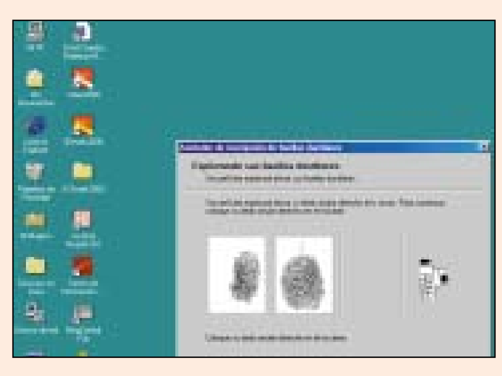
Por defecto, el sistema operativo realiza por sí mismo una copia diaria de este archivo. La aplicación que se encarga de esta tarea es *SCANREGW*. Además del registro del sistema, en los ficheros «.cab» (formato de compresión utilizado por Microsoft) que se



encuentran en la carpeta *C:\Windows\Sysbckup* se almacena otro tipo de ficheros como por ejemplo «System.ini» o «Win.ini». Para acceder al interior de estos repositorios tan sólo tendremos que pulsar con el botón derecho del ratón sobre el icono correspondiente y seleccionar *Ver*. Otra posible solución es disponer de algún programa compresor como Winzip, que permite el trabajo con estos ficheros.

PASO 2 Número de copias

Para aumentar el número de copias que se guardarán en este directorio especial, tendremos que especificarle a *SCAN-REGW* cuántos archivos conservar. Para ello abriremos el fichero «scanreg.ini» que se



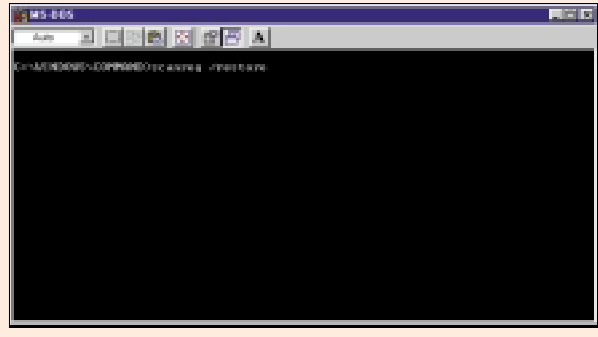
encuentra dentro de la carpeta *C:\Windows* con la aplicación *Bloc de notas*. A continuación editaremos el valor de *MaxBackupCopies* y le dotaremos con un nuevo número según nuestras preferencias. Al hacerse una copia diaria, lo que en realidad estaremos especificando es el número de días máximo al cual podemos volver atrás.

PASO 3 Restaurar un fichero

Restaurar cualquiera de los ficheros que se encuentran en el interior de los archivos CAB es tan sencillo como abrirlo y arrastrar y soltar el archivo en su carpeta originaria. Debemos tener en cuenta que esto es posible con casi todos los contenidos, a excepción del propio registro, para el que tendremos que utilizar una aplicación separada.

PASO 4 Restaurar el Registro

El motivo de que no podamos restaurar el Registro como el resto de los archivos viene dado por la intensa utilización del sistema operativo de este recurso. Para su restauración será necesario que iniciemos Windows 98 en modo *Solo Símbolo del Sistema*, a lo cual llegaremos pulsando la tecla «F8» al iniciar nuestro ordenador, cuando aparezca la frase *Iniciando Windows 98*. Ya dentro del sistema tendremos que teclear *scanreg/restore*. Aparecerá una lista con todas las copias disponibles, de la cual es conveniente seleccionar la más reciente. Si comprobamos que ésta no funciona, iremos descendiendo en antigüedad hasta encontrar alguna configuración correcta. Una nueva pulsación de la tecla «Intro» reiniciará nuestro equipo.



Internet, un gran peligro

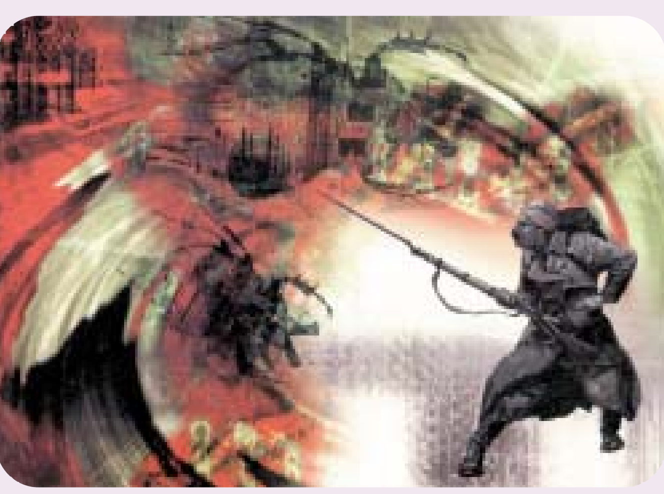
Muchos problemas los causa nuestra conexión a la Red

La Web no constituye un problema ético de divulgación de cuestionables temas, programas malignos, confidencialidades, etc., pero sí que representa un problema el mal uso que se hace de ella.

La no utilización de la red de redes nos eximirá completamente de todos sus inconvenientes, pero está claro que no merece la pena privarnos de tan suculento plato y dejar en el olvido la mayor fuente de información.

En la actualidad, existen diferentes aplicaciones que nos pueden ayudar a paliar el problema del lado oscuro del ciberespacio. Como ejemplo usaremos Guard Dog de McAfee, para mostrar una forma sencilla de filtrado de contenidos.

Una de las grandes preocupaciones, al margen de utilidad de los contenidos que podamos encontrar en la Internet, es la privacidad de nuestros datos en un entorno que se caracteriza por ser lo más parecido al salvaje oeste. Interceptar el correo electrónico es un juego de niños si disponemos de los medios suficientes para ello, algo que traerá de cabeza a aquellos que lo utilicen de forma indiscriminada.



Si uno de nuestras principales aficiones es pasar horas y horas conectado, empleando el chat como medio de comunicación o simplemente disfrutando de alguno de los juegos *online* disponibles hoy por hoy en el mercado, nos habremos dado cuenta de la importancia de la seguridad de nuestra red, aun cuando ésta se compone sólo de un equipo. Las aplicaciones que «cuelgan» nuestro equipo mientras estamos conectados o permiten el acceso a nuestro ordenado sin nuestro permiso abundan por todas partes.

Como muestra de cómo podemos aumentar la seguridad de nuestra conexión, os enseñaremos a desactivar algunos de los protocolos que Windows utiliza para compartir archivos, así como los medios más destacados para medir las vulnerabilidades de nuestro sistema. Dado que solucionar estos «agujeros» debiera ser una de nuestras prioridades, también os introduciremos en el manejo de uno de los programas que nos ayudarán a acabar con inoportunas intrusiones. Se trata de Type Personal Firewall, un cortafuegos personal que nos proporcionará un completo control sobre el estado de nuestras conexiones, incluso aquellas que a simple vista no podemos detectar.

MEDIO

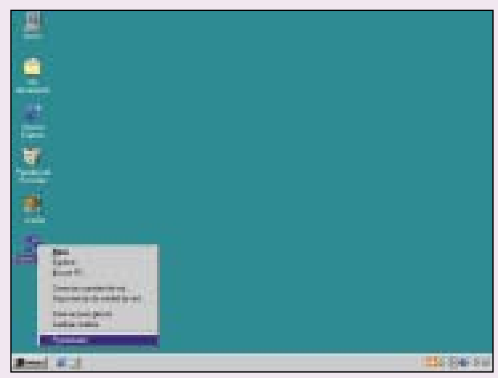
Elimina la NetBios

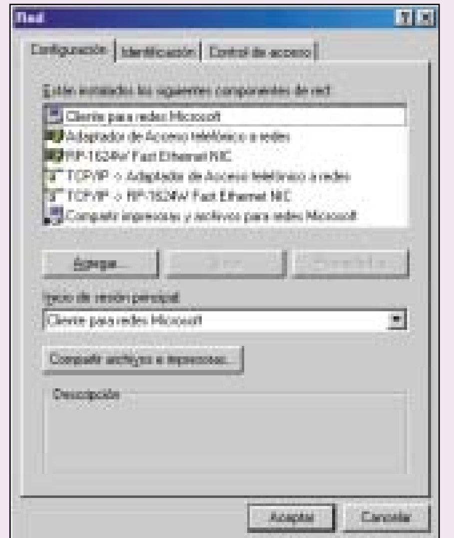
Haz que tus archivos sean invisibles vía Internet

En las primeras versiones de Windows 98 y Windows Me, corríamos el riesgo de hacer accesibles nuestros archivos al conectarnos a Internet. ¿Cómo evitarlo?

PASO 1 El protocolo NetBios

El problema lo encontramos en el protocolo llamado NetBios. Éste es el que permite compartir ficheros con el resto de nuestra red local; si está mal configurado, también permite compartir ficheros a través del acceso telefónico a redes, algo nada recomendable. Por otro lado, muchos usuarios ni siquiera utilizan una red local, por lo que esta función es del todo inútil. Si utilizamos un módem para acceder a Internet conviene deshabilitar este potencial agujero. Nuestro primer objetivo es localizar las propiedades de nuestra red, para lo que tendremos que pulsar con el botón derecho del ratón sobre el icono *Entorno de Red* y seleccionar la opción *Propiedades* del menú desplegable.



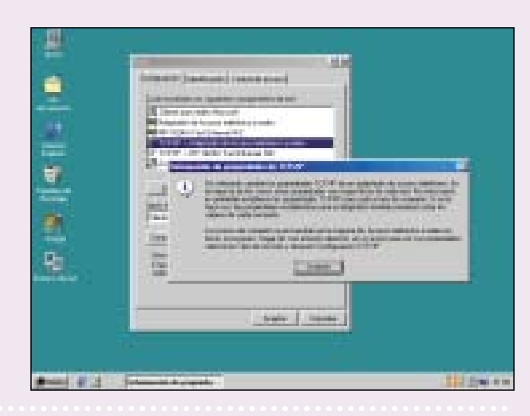


PASO 2 El Acceso telefónico a redes

Dentro de la nueva ventana que aparecerá en pantalla podremos ver todos los componente de la red, es decir, los protocolos, adaptadores y quién (y cómo) se utilizan. Debemos tener en cuenta que nuestra ventana no tiene que ser exactamente igual a la que os mostramos, ya que variará en función del hardware que tengamos instalado y los protocolos que utilicemos. Como protocolos «extra» que pueden aparecer nos referimos a IPX/SPX, que normalmente podemos eliminar con total seguridad de nuestra configuración pulsando sobre él y, a continuación, sobre el botón *Quitar* (si hacemos esto tendremos que reiniciar el equipo de nuevo). En esta ventana tendremos que localizar el protocolo *TCP/IP/Adaptador de Acceso telefónico a redes* y seleccionarlo, tras lo que pulsaremos sobre el botón *Propiedades*.

PASO 3 Aceptar cambios

Dependiendo de la versión de Windows que estemos utilizando, un nuevo cuadro de diálogo nos avisará de que cualquier cambio realizado a continuación puede afectar a nuestras futuras comunicaciones. Dado que los cambios que vamos a realizar no afectan a los parámetros de nuestro ISP (la empresa que nos proporciona el acceso a Internet), simplemente pulsaremos sobre *Aceptar*. De todas formas, es conveniente que tengas siempre a mano los datos del proveedor: pueden hacerte falta.



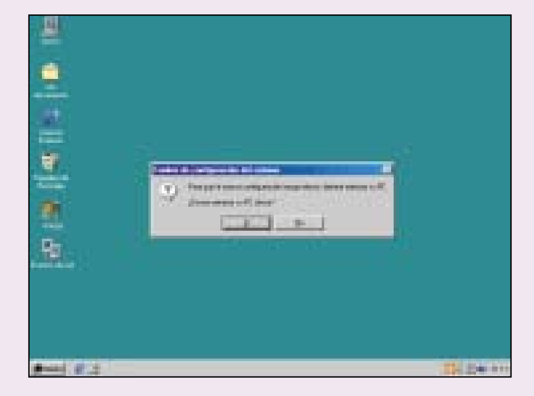
PASO 4 Deshabilitar NetBios

La ventana de propiedades del protocolo TCP/IP puede parecer bastante compleja a simple vista, aunque nosotros sólo nos centraremos en uno de los apartados. Las propiedades están clasificadas en varias carpetas que van desde *Dirección IP* hasta *Enlaces*, siendo precisamente esta última la que nos interesa. Pulsando sobre ella veremos para qué se utiliza realmente nuestro acceso telefónico a redes con unas pequeñas casillas marcadas a la izquierda de cada función. Para deshabilitar NetBios tan sólo tendremos que eliminar la marca a la izquierda de *Compartir impresoras y archivos para redes Microsoft*. Continuar con el proceso es tan simple como pulsar *Aceptar*.



PASO 4 Actualizar archivos

En ocasiones puede que Windows nos pida que introduzcamos el CD original de Windows 98. Una vez terminada la copia de archivos, si es necesaria, tendremos que reiniciar nuestro ordenador, tras lo cual nuestros archivos sólo serán visibles dentro de nuestra red local, evitando que ojos extraños cotilleen dentro de nuestras unidades de disco.



MEDIO

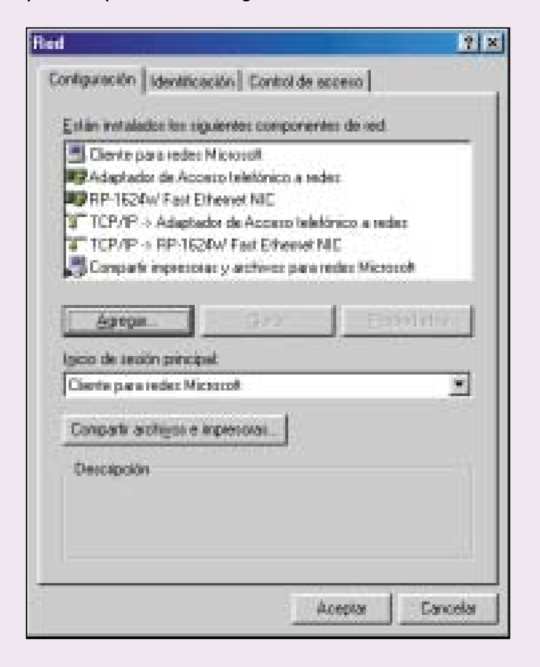
Introducir un nuevo protocolo

Sustituye NetBios por NetBeui

Tendremos que ocupar el lugar de NetBios con otro protocolo; si no, la amenaza de intromisión continuará pesando sobre el equipo.

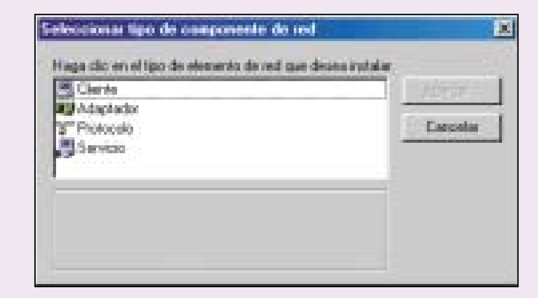
PASO 1 El puerto 139

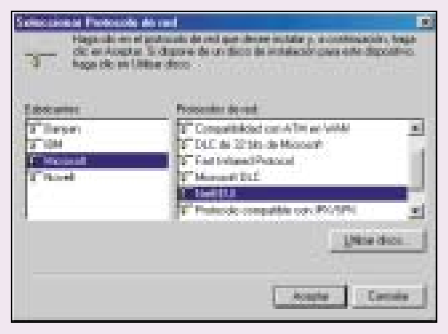
La solución que anteriormente os hemos descrito es tan sólo una aproximación a la situación ideal. Con ella conseguiremos no compartir archivos a través de la conexión a Internet, pero el puerto 139 sigue siendo toda una fuente de información para ojos no autorizados. Eliminar cualquier tipo de referencia a NetBios nos obligará a instalar otro protocolo diferente que se encargue de las comunicaciones en nuestra red interna, mientras que TCP/IP se encargará sólo de la conexión a Internet. Como antes, tendremos que acceder a la configuración de nuestra red y pulsar *Propiedades*.



PASO 2 Agregar un protocolo

A continuación añadiremos el protocolo que servirá para compartir los ordenadores dentro de nuestra red local. Para esto tendremos que añadir un nuevo componente a la lista de los ya existentes. Esto lo conseguiremos dirigiéndonos al botón *Agregar...* que se encuentra bajo la lista de los elementos que conforman la comunicación con otros ordenadores. Un cuadro de diálogo nos preguntará qué tipo de objeto queremos añadir, a lo que seleccionaremos *Protocolo* y continuaremos con *Aceptar*.

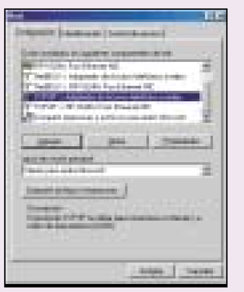




PASO 3 NetBeui

La lista de protocolos que podemos escoger es bastante amplia. Sin embargo, localizar el nuestro no es en absoluto complejo. En el cuadro de la izquierda seleccionaremos como fabricante a *Microsoft*, mientras que a su derecha optaremos por NetBeui. Éste es un protocolo muy sencillo, que no requiere configuración alguna y es perfectamente válido para nuestras necesidades: una pequeña red a la que no necesitamos acceder desde Internet. Si pulsamos el botón *Aceptar* continuaremos con el proceso, aunque dependiendo de la versión del sistema operativo que utilicemos éste requerirá que introduzcamos el CD-ROM original de Windows 98 para la copia de algunos archivos.

PASO 4 Editar propiedades



Los tres pasos que quedan tendremos que repetirlos tantas veces como ocasiones aparezca el protocolo TCP/IP en la lista de componentes de red. Con ello, deshabilitaremos la compartición de archivos utilizando este protocolo. En primer lugar seleccionaremos el componente adecuado y editaremos sus propiedades con el botón del mismo nombre. Debemos tener en cuenta que es muy importante actuar con todos y cada uno de los protocolos TCP/IP instalados, ya que de otra forma NetBios continuará instalado y, por lo tanto, habrá información privada al descubierto.



PASO 5 Desenlazar TCP/IP

Ya dentro de sus propiedades, abriremos la pestaña *Enlaces*. Dentro de ésta podremos ver todas las aplicaciones que se le dan a este protocolo (que a su vez está ligado a un adaptador de red). Nuestro cometido ahora consistirá en desenlazar el protocolo TCP/IP de todas las aplicaciones que aparezcan en este recuadro. Para ello, simplemente retiraremos las marcas que se encuentran a la derecha y aceptaremos.

PASO 6 Una configuración extraña

Windows, sorprendido ante nuestra «peculiar» configuración, insistirá en que liguemos el protocolo a alguna de sus funciones. Dado que nuestra intención es justamente la opuesta, contestaremos *No* y proseguiremos repitiendo este proceso si es necesario.



PASO 7 Reiniciar el equipo

Una vez hayamos concluido, tan sólo tendremos que pulsar sobre el botón *Aceptar* de la ventana *Propiedades de Red* para terminar. Será necesario que reiniciemos el ordenador e instalemos el protocolo NetBeui en aquellos ordenadores que vayan a compartir archivos con éste.

AVANZADO

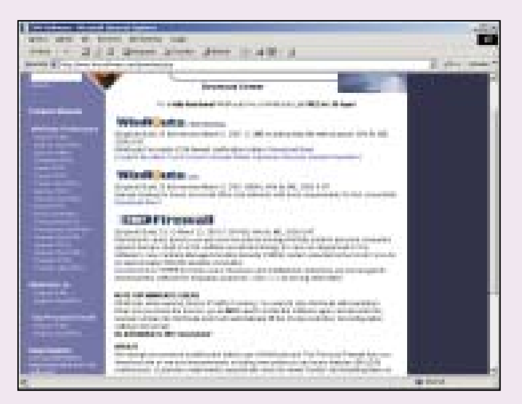
Un cortafuegos personal

Un Firewall software para controlar el acceso a datos

El control de nuestro flujo de datos, tanto de entrada como de salida, es muy importante para mantener nuestra integridad; veamos cómo manejar un Firewall.

PASO 1 Descargar el programa

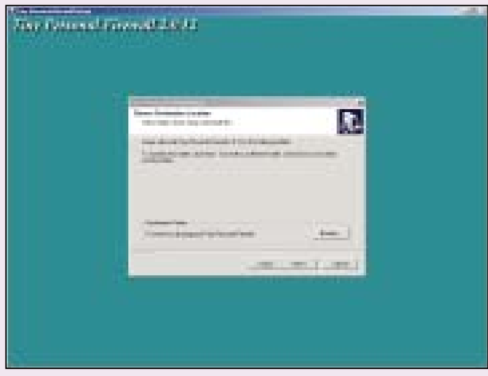
No por ser gratuito un producto es de menor calidad, ni más complicado de utilizar. Así lo demuestra Tiny Personal Firewall, la aplicación que usaremos para demostraros cómo



se configura un pequeño cortafuegos personal para evitar no sólo que ataquen nuestro ordenador desde el exterior, sino que algún troyano que se haya podido instalar envíe datos desde nuestro equipo al exterior. El primer paso es obvio, descargar el programa de la página web de la compañía (*www.tinysoftware.com/download.php*).

PASO 2 La instalación

Una vez descargado el programa, tan sólo tendremos que instalarlo. Éste es un proceso extremadamente simple. Únicamente deberemos pulsar dos veces sobre el ejecutable y especificar la ruta en la que se copiarán sus archivos. Dado



que el programa utiliza algunos componentes «críticos» dentro del sistema, será necesario que reiniciemos el equipo, tras lo cual el cortafuegos comenzará a funcionar.

PASO 3 Direcciones fiables

La primera noticia que veremos del funcionamiento del cortafuegos será nada más arrancar Windows. El programa,



al detectar que nuestro ordenador comienza a enviar paquetes NetBios, nos avisará. Al ser la primera vez que detecta tráfico, nos preguntará si deseamos establecer un rango de direcciones fiables. Este rango de direcciones IP será normalmente el de nuestra red local. De esta forma, podemos obligar al cortafuegos a fiarse de los paquetes que van y vienen a esas direcciones. La aplicación normalmente será capaz de detectar este valor, con lo que tan sólo tendremos que seleccionar la segunda opción y pulsar *Aceptar*.

PASO 4 Nivel de seguridad

A continuación, tendremos que establecer el nivel de seguridad que deseamos para nuestro equipo. Para ello, tan sólo tendremos que dirigirnos a un icono que se



sitúa a la izquierda del reloj, en nuestra barra de tareas. Pulsando con el botón derecho sobre éste y seleccionando *Firewall Administration*, aparecerá una ventana en la que podemos seleccionar tres modos de protección. El más bajo (*Don't Bother Me*) no hará preguntas y todas aquellas conexiones que el cortafuego no conozca serán permitidas. El más alto (*Cut Me off*), por su parte, hace justo lo contrario, evita cualquier tipo de tráfico, con lo que no dispondremos de conexión a la red. Lo más recomendable es seleccionar el nivel intermedio (*Ask Me First*), que pedirá confirmación antes de conectarse a cualquier parte que no esté especificada en las reglas.

PASO 5 El permiso

Tal cual está configurado el cortafuegos, al navegar veremos cómo, al acceder a cualquier página web, la aplicación nos pregunta si permitir la conexión o rechazarla. Lo mismo ocurrirá con las demás aplicaciones que utilice la red, con lo que cualquier troyano será fácilmente detectado. En la ventana aparecerá el nombre de la aplicación que necesita establecer una conexión, junto con la dirección IP del servidor (o equipo) remoto y el puerto.

Si escogemos *Permit* se establecerá la cone-



xión. Si además hemos marcado la casilla *Create apropiate filter rule and don't ask me again*, el propio cortafuegos creará un regla que permitirá a la aplicación seguir funcionando sin molestarnos más.

El botón *Deny* funciona justo al contrario, es decir, denegando la conexión. Debemos tener mucho cuidado a la hora de crear estas reglas y comprobar que realmente nos fiamos de esa aplicación para conectarse «a su gusto».

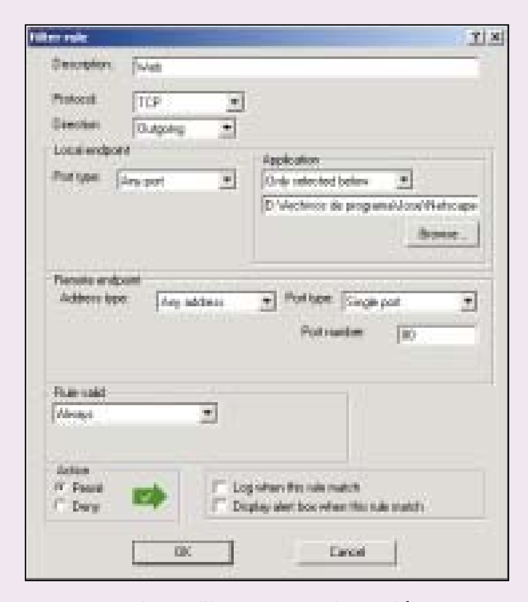
PASO 6 Reglas de conexión



Para crear una de estas reglas, tan sólo tendremos que dirigirnos al menú del paso número 4 y pulsar sobre el botón *Advanced*. En la pantalla *Firewall Configuration* veremos una lista con todas las reglas. Los símbolos utilizados son bastante explicativos: a la izquierda veremos una marca que indica si esa regla está o no en vigencia y junto a ella una pequeña flecha. Si ésta es verde, quiere decir que se permite la conexión; por el contrario, si es de color rojo se impedirá. La dirección de la flecha (izquierda, derecha o ambas) indica en qué sentido se permite (o deniega, según el color) la conexión. Si mira hacia la izquierda es una conexión realizada desde fuera, es decir, desde otro ordenador. Si mira hacia la derecha indica un intento de conexión a otro ordenador externo. Ambas de forma simultánea indican que se permite (o deniega) cualquiera de los dos casos. Podemos eliminar, añadir o editar estas reglas con los botones situados bajo la lista. Pulsaremos el botón *Add* para crear una nueva.

PASO 7 Conectarse con el puerto 80

Éste es sólo un ejemplo de regla que permitirá a cualquier aplicación conectarse a un servidor utilizando el puerto 80 (puerto de los servidores web). No es en absoluto el más seguro pero bastará para que veamos cómo se crea una regla que realmente nos proteja de amenazas conocidas. Una vez hayamos realizado una descripción apropiada para esta regla en el primer recuadro disponible, tendremos que escoger el tipo de protocolo que vamos a permitir y la dirección. En nuestro caso utilizaremos TCP como protocolo de salida (nosotros iniciamos la conexión). El puerto de conexión local es indiferente, aunque no la aplicación. Si queremos una seguridad decente tendremos que especificar en la casilla la aplicación a la que se le permitirá utilizar esta regla. En la casilla *Application* seleccionaremos *Only Selected Below* y con el botón *Browse* apuntaremos a la ruta en la cual se encuentra el programa (en nuestro caso Netscape 6). Tan sólo queda por definir a qué tipo de servidores vamos a permitir el acceso. Dado que no nos interesa el servidor, deberemos



escoger en la casilla *Port type:* la opción *Single port* y escribir en la inferior en número 80. Pulsando *Ok* habremos creado nuestra primera regla, algo que poco a poco iremos haciendo con más práctica.

BÁSICO

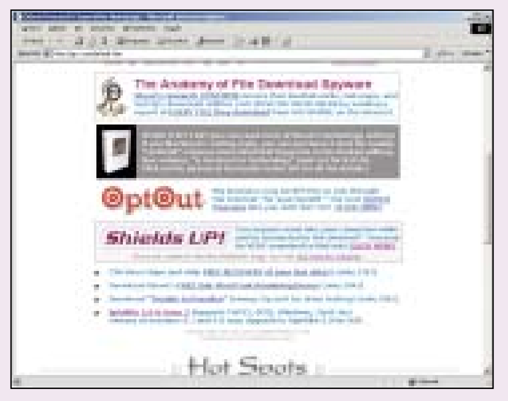
Busca tus fallos

Es importante conocer los puntos flacos de nuestro PC

Escanear el equipo con programas como Shields Up! nos ayudará a conocer nuestros propios «agujeros» de seguridad.

PASO 1 Descargarlo de Internet

Nuestro primer objetivo es, obviamente, conectarnos a una de las páginas existentes en Internet. Necesitaremos estar conectados a la Red antes de disponer



de este acceso, por lo que tendremos que utilizar nuestro *Acceso telefónico a Redes* o encender el dispositivo que nos «engancha» a Internet. Una vez dentro, tan sólo será necesario que abramos la página web utilizando Internet Explorer o Netscape Comunicator, dependiendo del programa que utilicemos habitualmente. A continuación, tan sólo tendremos que introducir la dirección de la página en la barra reservada a tal efecto. En nuestro caso utilizaremos uno de los servicios más populares, educativos y gratuitos disponibles en la red de redes, Shields Up! Éste se encuentra en la dirección *http://grc.com*, en cuya página tendremos que seleccionar el *banner* correspondiente al servicio.

PASO 2 Una conexión segura

Al pulsar sobre el gráfico correspondiente aparecerá una nueva ventana que nos anuncia el paso a una conexión segura.



Una vez pulsemos el botón *Aceptar* toda la información que enviemos a través de este navegador, en nuestro caso Internet Explorer, estará cifrada. No es más que una medida de seguridad que evitará que posibles «cotillas» de la red «escuchen» todo lo que enviamos al servidor. De esta forma, aun cuando la página encuentre algún fallo de seguridad en nuestro equipo, sólo nosotros podremos hacer uso de esta información para intentar solventar cualquier problema.

PASO 3 Pasos previos

Si nos conectamos utilizando un *Acceso telefónico a Redes* convencional, por ejemplo con un módem analógico, RDSI o un módem ADSL, nuestra dirección IP **pública** (la que todo el



mundo puede ver en Internet) coincidirá con la de nuestro ordenador. Sin embargo, si utilizamos algún tipo de *router*, *proxy* o similar, puede que ésta no coincida. Como las pruebas se basan en la dirección IP de nuestro ordenador, y para asegurarnos de que se realizan correctamente, conviene que nos descarguemos una pequeña aplicación llamada *IP Agent*. Para esto pulsaremos sobre el enlace *Free IP Agent* o *quick to download*. Si utilizamos Internet Explorer, tendremos una opción que nos permite ejecutar directamente el programa desde Internet. Si utilizamos Netscape, será necesario que guardemos antes el programa en una carpeta de nuestro disco duro y posteriormente lo ejecutemos. Si Internet Explorer nos advierte de algún problema de seguridad, como por ejemplo que no puede comprobar la firma, podemos ignorarlo tranquilamente.

PASO 4 Conexión con la página

En el caso de que ejecutáramos el programa descargado en el paso anterior, aparecerá en nuestra pantalla una pequeña ventana que indica la dirección IP de nuestro equipo. Para continuar con la prueba,



tan sólo tendremos que pulsar el botón *Test My Shields* (prueba mis escudos) para continuar. El pequeño programa se conectará a la página automáticamente y enviará nuestra dirección real para ser probada.

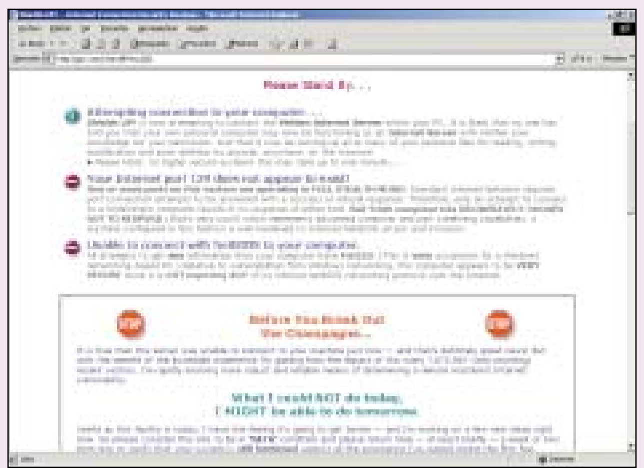


PASO 5 Números «privados»

Si nuestra dirección de red pertenece a algunos de los rangos de números definidos como «privados», estaremos de suerte, ya que es imposible acceder desde el exterior a nuestro ordenador. El «truco» consiste en evitar que cualquier tipo de paquete sea capaz de encontrar un camino hacia nuestro ordenador. En este caso, las pruebas habrán concluido, ya que nuestro equipo no puede ser alcanzado desde el exterior, al menos de una forma convencional, y se considera completamente seguro.

PASO 6 Posibles problemas

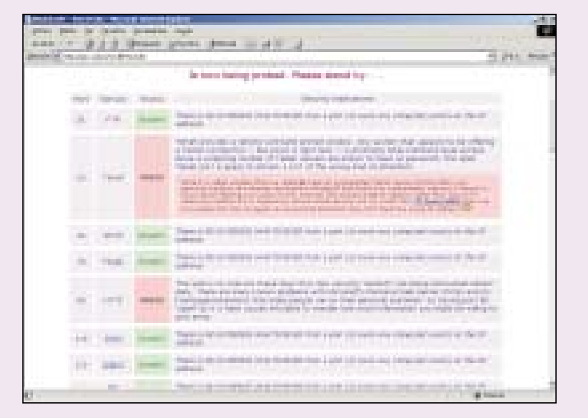
Lo más probable es que *IP Agent* haya detectado que nuestra dirección es «vulnerable», o que hayamos decidido continuar sin este programa escogiendo alguno de los dos métodos de prueba que se muestran en la pági-



na (*Test My Shields!* o *Probe My Ports!*, ambos botones rojos perfectamente visibles en la web). Comenzaremos con el primero de los sistemas, *Test My Shields!*, haciendo un clic de ratón sobre esta imagen. Automáticamente aparecerá en la pantalla de nuestro navegador la dirección IP pública de nuestro sistema y, bajo ésta, una descripción detallada de todos los problemas que la página va encontrando poco a poco. Se trata de un primer análisis, que determinará la seguridad de nuestro sistema «a primera vista», aunque desde luego no sea definitivo. Una vez hayamos anotado todos los posibles problemas existentes (y soluciones sugeridas), podremos continuar con la prueba pulsando el botón *Probe My Ports!* que se encuentra bajo las descripciones.

PASO 7 Estado de los puertos

Dentro de esta página aparecerá de nuevo nuestra dirección IP. Sin embargo, bajo ésta veremos una lista con los puertos principales de nuestro ordenador. A la derecha de éstos, veremos su estado, *Stealth!*, *Close* u *Open*. Bajo la enumeración de puertos veremos una explicación detallada del significado de cada uno de los estados. No obstante, debemos tener en cuenta que cuantos más puertos tengamos abiertos más posibilidades existen de que alguien intente aprovecharse de nuestra debilidad para acceder a nuestro equipo de forma ilícita.



BÁSICO

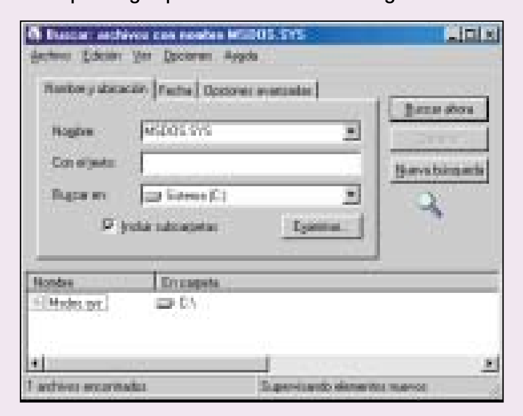
Filtrar los contenidos de Internet con Guard Dog

Un perro guardián

Sexo, violencia, terrorismo, manifestaciones racistas, etc., son temas que se encuentran al alcance de cualquiera en Internet. Este programa de McAfee nos ayudará a evitarlos.

PASO 1 Diferentes cuentas

Después de una rápida instalación, en la que tan sólo deberemos seguir los pasos perfectamente detallados durante el proceso, tenemos que dar de alta una cuenta de usuario de administrador, que será quien tenga total privilegio para cambiar las configuraciones



de todos los usuarios. Desde su menú de inicio podemos crear diferentes cuentas para cada uno de los sujetos que accederán al ordenador. Lo primero que introduciremos serán los nombres y las contraseñas de acceso de cada uno. Esta operación se realizará inmediatamente después de hacer la instalación, justo cuando reiniciemos el equipo. Posteriormente se introducirá el nivel de seguridad, que se puede elegir entre mínimo, máximo o configurable por el usuario.

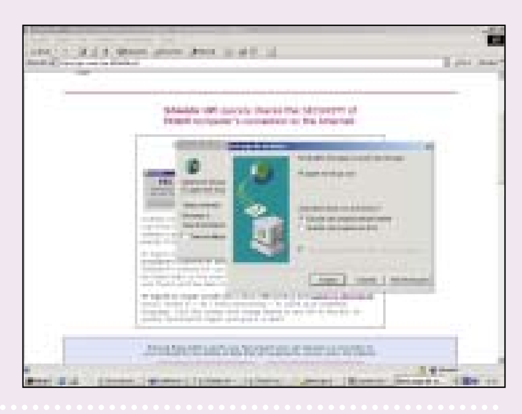
PASO 2 Niveles de seguridad

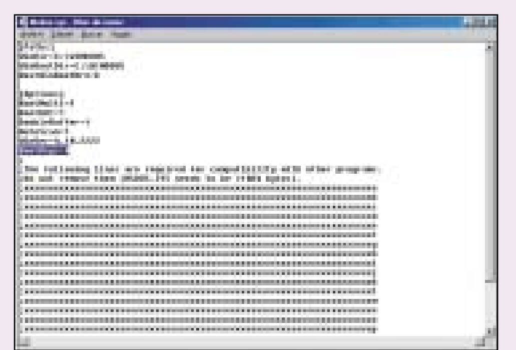
Daremos de alta a los usuarios que deseemos, indicando los privilegios de los que podrá disfrutar y asociándolo a una contraseña determinada. Se podrá dar derecho de autoadministrador a las personas que se consideren responsables de sus actos, para que puedan configurar ellos mismos las opciones de privacidad y protección. Deberemos indicar el nivel de seguridad de la cuenta, pudiendo elegir entre máxima, mínima, configurable, o incluso adoptar la de otro usuario ya creado con anterioridad.



PASO 3 Limitación de contenidos

A continuación, introduciremos las restricciones horarias que permitirán el acceso a Internet, las cuales están en forma de franja para cada uno de los días de la semana. El ratio de contenidos especificará la madurez de la persona, que en escala se sucederá desde los más jovencitos, eliminando la posibilidad de recibir mensajes con determinadas palabras o frases, hasta la posibilidad de no filtrar ninguno de éstos tanto en la web como en las famosas charlas *on-line* o *chats*.





PASO 4 Datos secretos

Después de esto, se indicará la información privada que desearemos que se mantenga en secreto y que no se podrá transmitir a menos que demos nuestra aprobación. Se podrá incluir nombres, apellidos, direcciones, teléfono, etc. En el apartado de *Protección*, indicaremos la información que Guard Dog protegerá, como cuentas de tarjetas Visa, etc. Tenemos la posibilidad de almacenar sitios web asociados a un nombre de usuario y una contraseña, y protegerlas en un lugar seguro de forma encriptada.

PASO 5 Realizar cambios

Acabado el proceso, el administrador podrá realizar cualquier cambio de una forma rápida, editando el usuario desde el menú principal. Entre otras opciones, tenemos la posibilidad de configurar el filtro de contenidos en diferentes campos, como pueden ser los de sexo, violencia, racismo, etc. Cada vez que se inicie el equipo, se nos pedirá que metamos el nombre de usuario y su contraseña asociada, pues de esta forma se tendrá la identificación segura del usuario en cada momento.

Obviamente, este tipo de guardianes no es completamente infalible, como sucede con casi todos los elementos de seguridad que son software. En cualquier caso, este perro guardián es muy efectivo para mantener a los más pequeños alejados de contenidos poco aconsejables.

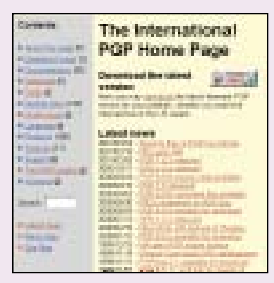


MEDIO

Firmas digitales

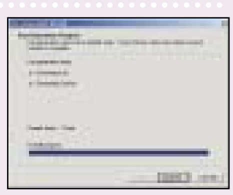
Un elemento de identificación cada vez más extendido

El programa PGP nos permitirá tanto este proceso como el de encriptación de e-mail que veremos más adelante.



PASO 1 Obtención del programa

En primera instancia tendremos que descargarnos e instalar el programa PGPi (la letra «i» especifica que se trata de la versión internacional, no sujeta a las reglas de exportación americana). Podremos bajarnos la última versión (en este momento la 7.0.3) desde la página www.pgpi.org.



PASO 2 Creación de clave privada

Una vez arrancado el ordenador, un asistente nos guiará en el proceso de creación de una clave privada. Será necesario que introduzcamos nuestro nombre y dirección de correo electrónico. A continuación tendremos que especificar una frase, que será la que proteja la integridad de nuestra llave privada.



PASO 3 Selección de opciones

Dado que PGP no es compatible con todos los programas, utilizaremos un método que funcionará con casi la totalidad de ellos. Tendremos que dirigirnos al icono de PGP situado en nuestra barra de tareas, pulsar con el botón derecho para abrir el menú *Options* y, dentro, *Hotkeys*. En el siguiente panel activaremos las opciones *Encrypt current window*, *Sign current window*, *Encrypt & Sign current Window* y *Encrypt & Verify current window*.

PASO 4 El cifrado del correo

Para cifrar o firmar un mail, tan sólo tendremos que abrir un nuevo mensaje. Después de escribir el texto, tendremos que seleccionarlo al completo y pulsar alguna de las siguientes combinaciones de teclas, según queramos firmar, cifrar o ambos respectivamente: «Control+Shift+S», «Control+Shift+E», «Control+Shift+C». Una nueva ventana nos pedirá que introduzcamos la frase que protege nuestra clave privada. Si escogimos cifrar el mensaje se nos pedirá, además, que introduzcamos los destinatarios de éste, cuyas llaves públicas deberán estar almacenadas en nuestro ordenador.

PASO 5 Comprobación

Comprobar la validez de un mensaje utilizando la firma, o descifrarlo, es un proceso muy similar. Tan sólo tendremos que abrir el mensaje, seleccionar el contenido al completo y pulsar la combinación de teclas «Control+Shift+D». Una nueva ventana nos mostrará si el mensaje es válido (si estaba firmado) y lo descifrará si es oportuno.

GLOSARIO DE TÉRMINOS

A primera vista los términos que se utilizan en todo lo concerniente al tema de seguridad pueden parecer complicados, pero por suerte no es así. Aquí, en nuestro habitual glosario, definimos algunos de ellos que nos servirán para entender mejor todos los pasos a paso y trucos que en este libro os proponemos.

Agujero de seguridad: Posible flanco por el cual podemos sufrir un ataque a nuestros equipos. Existen de muchas clases, desde los que permiten la salida de datos de nuestro ordenador de forma no autorizada hasta los que impiden que alguno de los programas, e incluso el ordenador al completo, cumplan con su objetivo (agujeros de seguridad llamados DoS, de *Denial of Service*).

Atributos de ficheros: Los atributos de los ficheros son algunas de sus propiedades que se pueden modificar fácilmente desde el sistema.



Backup: Copia de seguridad que sirve para poder restaurar información en caso de que se nos haya perdido o deteriorado.

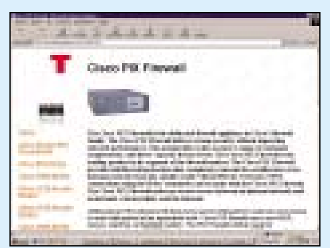
Biometría: Ciencia que se dedica a identificar y medir determinados rasgos que se encuentran en el ser humano. Los lectores de huellas dactilares, de iris y los reconocedores de voz son algunos ejemplos de productos biométricos. Sus grandes posibilidades en el campo de la identificación personal son incuestionables.

BIOS: De las siglas *Basic Input Output System*, es un chip que traduce información entre el software y el hardware del sistema. Además, guarda los parámetros de configuración de algunos componentes, como son los discos duros, etc.

Encriptación: Proceso por el cual se cifra un archivo para que sea inteligible por otros aparatos o personas. Se hace en base a una serie de operaciones, que descolocan los datos y cuyo proceso inverso las vuelve a hacer servibles.

Faja de conexión: Conjunto de conductores que se disponen de forma paralela y que en su conjunto tiene forma de lazo o faja.

Firewall: Este término viene del inglés y quiere decir cortafuegos. Es un mecanismo que impone una barrera en un flujo de datos. Existen firewalls tanto hardware como software; su misión es el de controlar la información que sale o entra de un determinado dispositivo. La gran mayoría funciona utilizando una serie de reglas que impiden, o permiten, una conexión, en función de sus características.



Firmas digitales: Es el equivalente a la firma que ponemos en un papel para rubicar nuestra conformidad con lo escrito. Las firmas digitales actúan a modo de notarios electrónicos identificando que un correo, o cualquier intercambio de información, está realizada por el propietario de la firma.

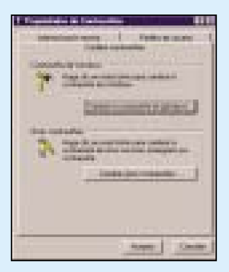
ISP: *Internet Service Provider*, son aquellas empresas que se dedican a ofrecer servicios de conexión a Internet. Cuando nos «enganchamos» a la red de redes, marcamos un número telefónico a través del cual tenemos acceso al resto de las máquinas que configuran Internet. Este número de teléfono es el del ISP.

Jumpers: Esta palabra inglesa quiere significar puente. Los *jumpers* son unas pequeñas piezas de plástico en cuyo

interior se encuentra un material conductor capaz de hacer cortocircuitos. Éstos son fácilmente extraíbles, por lo que son una buena solución para realizar configuraciones hardware, pues ubicándolos en determinados sitios de aparatos electrónicos, podemos proporcionar información al equipo.

NetBios: Protocolo que permite que los archivos de una red de ordenadores puedan ser compartidos.

Password: Una *password*, del inglés paso (*pass*) y palabra (*word*), es una clave o contraseña que se introduce para verificar la identificación



de un individuo determinado. Debe ser conocida sólo por las personas que tengan privilegios, pues si pasa a ser de dominio público pierde toda su utilidad.

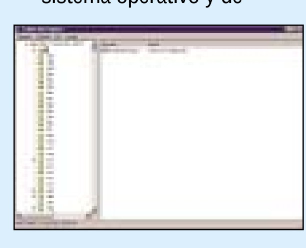
Protocolo: Para que se pueda producir una comunicación, es necesario que se den una serie de factores. Éstos son el emisor, que es quien envía el mensaje, el receptor, que es quien lo recibe, y el canal de transmisión. El mensaje es enviado con una codificación que debe conocer el receptor; si no, no habría entendimiento. Esta codificación, que en el lenguaje humano es nuestro idioma, es un protocolo. Es decir, unas reglas que definen el significado de la información.

Proxy: Programa que, una vez que se ha instalado en un equipo, permite que otros conectados a él puedan tener acceso a Internet mediante una sola conexión. El problema que tienen este método, que ahorra enlaces y por lo tanto llamadas y dinero, es que cuanto mayor es el número de usuarios nutriéndose de Interntet, más lento es el flujo de transferencia de Información.

Puerto: Número que define la aplicación a la que va destinada la conexión. Es uno de los factores que define una conexión. Ésta está determinada por un origen (dirección IP y puerto) y un destino (dirección IP y puerto).

Red local: Conjunto de ordenadores conectados entre sí en una corta distancia de espacio. Las limitaciones del cableado hacen que para enlazar dos equipos que se encuentran muy separados tengamos que usar la línea telefónica o similar. Una red local utiliza unos cables que permiten una alta velocidad de transferencia en espacios reducidos.

Registro de Windows: Aquí se guarda un montón de parámetros de configuración del sistema operativo y de



los usuarios. Cada vez que se inicia el equipo, todas las variables de personalización de este registro se cargan.

ROM: *Read only Memory*, memoria de sólo lectura. Es un componente electrónico que almacena bits pero, a diferencia de la conocida RAM, sólo permite ser escrita una sola vez, aunque se pueda leer un número indefinido de veces.

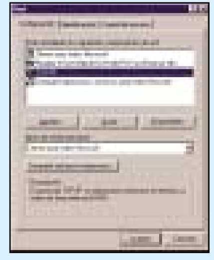
Router: Aparato que servirá de pasarela entre distintos tipos de redes.

SETUP: Interfaz gráfica de la BIOS que nos permite interaccionar con ella para cambiar los parámetros configurables por el usuario.

Slot: Conector que permite enchufar y desenchufar dispositivos como microprocesadores o tarjetas, y que tiene la particularidad de albergar los componentes de manera perpendicular a su soporte.

Socket: Al igual que el Slot, es un zócalo; sin embargo, su formato permite que el componente sea ubicado de forma paralela al soporte.

TCP/IP: Protocolos que se utilizan habitualmente en la conexión a Internet. El nombre hace referencia a



dos protocolos, aunque cuando nos referimos a ellos normalmente se engloban dentro otros protocolos como UDP.



Editado por VNU Business Publications España. ***computer*!dea. Director:** Rufino Contreras. **Coordinador:** Rafael María Claudín. **Redactores y colaboradores:** Raúl Rubio Seguer, José Plana Mario, Fernando Reinlein, Susana Harari, Elena Julve y Javier Renovell. **Jefe de Arte y portada:** Fco. Javier Herrero. **Maquetación:** Ismael Ortuño. **Director de Producción:** Agustín Palomino. **Imprenta:** Cobrhi. **Suplemento especial de *computer*!dea** número 5. Mayo 2001.



San Sotero, 8 - 4ª planta. 28037 Madrid. Teléfono: 913 137 900. Fax: 913 273 704
Avda. Pompeu Fabra, 10 - bajos. 08024 Barcelona. Teléfono: 932 846 100. Fax: 932 103 052